III. REMARKS

1. Claims 1, 4-6, 9-11 and 15-18 are amended. Claims 1-23 are pending in this Application.

2. Applicant submits that the Final Rejection of the claims is premature. It has not been indicated by the Examiner that the new grounds of rejection were necessitated by Applicant's amendments of the claims nor is the Final Rejection based on information submitted in an information disclosure statement. Rather this Final Rejection of the claims is based on prior art not of record. The finality of this rejection should be withdrawn. (See M.P.E.P. § 706.07(a)).

3. Claims 1, 2, 4-7, 9-13 and 15-23 are not anticipated by Debbins et al., U.S. Patent No. 6,331,776 ("Debbins") under 35 U.S.C. 102(e). Claim 1 recites a module located within the intermediate network, through which all data transferring between the local network and the remote network must pass, the module being configured to provide indirect remote access to at least one semiconductor processing tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool. Debbins does not disclose or suggest at least these features.

Debbins discloses a method for the remote operation and servicing of a magnetic resonance imaging (MRI) system. The method includes establishing a communication connection over a network between the MRI system and the remote facility to provide remote services to the MRI system (Col. 2, L. 33-39). The service system (1010) of Fig. 4 provides remote service to diagnostic systems (1012). The diagnostic systems (1012) are

serviced from a centralized service facility (1022) (Col. 9, L. 29-41). As shown in Fig. 4 of Debbins, the diagnostic systems (1012) communicate with the centralized service facility (1022) over a network (1080) (Col. 10, L. 58-60). A plurality of field service units (1024) may be coupled in the service system for transmitting service requests, verifying service status and transmitting service data (Col. 9, L. 29-44). As shown in Fig. 4, the remote service units (1024) also communicate with the centralized service facility (1022) over the network (1080). Remote services include remote monitoring, remote system control, immediate file access from remote locations, remote file storage and archiving, remote resource pooling, remote recording and remote high speed computations (Col. 9, L. 47-51). A management station (1070) may link more than one medical diagnostic system in a single facility or location (Col. 10, L. 30-36). The management station (1070) is connected to the work station (1072) that is linked to the service facility (1022) via the remote access network (1080) (Col. 10, L. 58-60). Thus Debbins does not disclose or suggests a first network permitting data transfer between a local network and an intermediate network and a second network permitting data transfer between the intermediate network and a remote network as called for in claim 1. Debbins only discloses a single "remote access network (1080)" that links the "service facility (1022)" to the "workstation (1072) and field service units (1024)" (Col. 10, L. 58-60). Debbins also does not disclose or suggest a module located within the intermediate network, through which all data transferring between the local network and the remote network must pass, the module being configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool.

The Examiner suggests that the automated service unit (1136) as disclosed at Column 13, Lines 59-66 of Debbins reads on the module located within the intermediate network as recited in Applicant's claim 1. The Applicant respectfully disagrees. The automated service unit (1136) of Debbins is located within the service facility (1022) and not an intermediate network (Col. 13, L. 59-60). Furthermore, the automated service unit only responds to "certain" service requests. There is no disclosure or suggestion in Debbins that "all" data must pass through the automated service unit. In Applicant's invention "all data" transferring between the local network and the remote network must pass through the module.

In addition, the automated service unit it is not disclosed as being configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool as recited in claim 1.

In Debbins, the MRIs, workstations (1072) and field service units (1024) may be linked to service facility (1022) through a remote access network (1080) such as the internet. Data may be exchanged between the diagnostic systems, field service units and the remote service facility (1022) in accordance with Internet Protocol (IP) or Transmission Control Protocol (TCP) (Col. 10, L. 58 - Col. 11, L. 6). Messages, service requests and data are received at the service facility (1022) through communications port (1082) which transmits this data to the service center processing system (1084) (Col. 11, L. 7-12). Platform (1090) is provided within each diagnostic system (1012) (i.e. the MRI system) and enables a direct interface between the service facility (1022) and the control circuitry of the

individual scanners of the diagnostic system (1012) (Col. 11, L. 29-61). As can also be seen in Figure 4, the service facility (1022) is connected directly to the diagnostic equipment (CT system 1016 and MRI system 1014) through communications port (1048, 1032). This is not the same as the module being configured to provide indirect remote access to a tool located in the local network as recited in claim 1.

In addition, in Debbins, prevention of unauthorized access is only disclosed with respect to the service facility through the use of firewalls within the processing system (1084) (Col. 11, L. 62-66). This is not the same as the module being configured to prevent an unauthorized interception of communications between the local network and the remote network related to the tool as called for in claim 1. Further, nowhere is there any disclosure or suggestion in Debbins of a module located within the intermediate network, through which all data transferring between the local network and the remote network must pass. Debbins only discloses that the service facility (1022) is connected to the diagnostic systems (1012) and its related equipment through the internet (Col. 10, L. 58-64).

Claim 1 is not anticipated by Debbins because Debbins fails to disclose or suggest a module located within the intermediate network, through which all data transferring between the local network and the remote network must pass, the module being configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool.

Furthermore, claim 1 recites a local network comprising at least one semiconductor processing tool and semiconductor processing

tool monitoring equipment, an intermediate network comprising an equipment diagnostic monitoring system configured to monitor and analyze the at least one semiconductor processing tool and a remote network comprising remote control equipment configured to allow a user remote access to the at least one semiconductor processing tool. Nowhere does Debbins disclose or suggest a network having at least one semiconductor processing tool or an equipment diagnostic monitoring system to monitor and analyze the at least one semiconductor processing tool.

Debbins is concerned with the remote control of medical diagnostic systems such as MRIs and CT systems for diagnosing humans (Fig. 4; Col. 2, L. 7-30), not semiconductor processing tools as recited in claim 1. In addition, Debbins does not disclose an equipment diagnostic monitoring system configured to monitor and analyze the at least one semiconductor processing tool. In Debbins, the service facility (1022) receives messages, service requests and data from the users of the medical diagnostic system (Col. 11, L. 7-12). This is not what is claimed in claim 1. In claim 1, an intermediate network comprising an equipment diagnostic monitoring system is configured to monitor and analyze the at least one semiconductor processing tool and a remote network comprising remote control equipment is configured to allow a user remote access to the at least one semiconductor processing tool. In Debbins, there is no equipment diagnostic monitoring system in an intermediate network. The service facility (1022) only acts upon the medical diagnostic equipment upon request (i.e. after receiving a service request from an operator of the diagnostic equipment)(Col. 11, L. 7-12) and in the context of the geometry information related to the images acquired by that equipment for diagnosing humans (Col. 2, L. 33 - Col. 3, L. 50). There is no

disclosure in Debbins of diagnosing the medical diagnostic equipment itself.

Therefore, claim 1 is patentable over Debbins for the additional reason that Debbins fails to disclose or suggest a local network comprising at least one semiconductor processing tool and semiconductor processing tool monitoring equipment, an intermediate network comprising an equipment diagnostic monitoring system configured to monitor and analyze the at least one semiconductor processing tool and a remote network comprising remote control equipment configured to allow a user remote access to the at least one semiconductor processing tool.

Claim 6 recites a module located within the intermediate network, through which all data transferring between the local network and the remote network must pass, wherein the data is selectively passed between the local network and the remote network depending on a set of predetermined criteria applied by the intermediate network and, the module being configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool.

Claim 11 recites a second network interface device enabling data transfer between a remote network and the intermediate network, the intermediate network is configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool.

Claims 6 and 11 are not anticipated by Debbins for reasons similar to those described above with respect to claim 1.

Claims 2, 4, 5, 7, 9, 10, 12, 13 and 15-23 are patentable by reason of their respective dependencies.

4. Claims 3, 8 and 14 are patentable under 35 U.S.C. 103(a) over Debbins in view of Reid et al., U.S. Patent No. 6,182,226 ("Reid"). For the reasons described above, Debbins does not disclose or suggest the features of claims 1, 6 and 11 from which claims 3, 8 and 14 depend.

Reid also fails to disclose or suggest the features of claims 1, 6 and 11. As described in the response to the prior office action, the arguments of which are incorporated herein by reference in their entirety, Reid does not suggest or disclose a module located within the intermediate network as in claim 1 of the present application. In Reid, there is an internal network (32), which is broken up into regions, that is connected to an external network (36). Communications between these two networks is restricted by firewall (34). Communication between internal network (32) and server 42 is also restricted by firewall (34). As such, in Reid, the communication between two networks (32, 36) does not pass through an intermediate network as claimed in claim 1 of the present application. In addition, nowhere is it disclosed in Reid that the module being configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool. There is no disclosure of an intermediate network in Reid.

Neither Debbins nor Reid, individually or in combination, disclose or suggest a module located within the intermediate network, through which all data transferring between the local network and the remote network must pass, the module being

configured to provide indirect remote access to a tool located in the local network and to prevent an unauthorized interception of communications between the local network and the remote network related to the tool as recited in claim 1. Therefore, Claim 1 is patentable over Debbins in view of Reid.

Reid does not disclose or suggest the features of claims 6 and 11 for reasons similar to those described above with respect to claim 1. Accordingly, Reid does not suggest or disclose the features of claims 6 or 11 for reasons similar to those above. Claims 3, 8 and 14 are patentable over the combination of Debbins and Reid by reason of their respective dependencies.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Geza C. Ziegler, Jr.
Reg. No. 44,004

9 JAN 2006
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted by facsimile to (571) 273-8300 the date indicated below, addressed to the Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Date: January 9, 2006 Signature: Meaghan Bayl
Person Making Deposit